User Manual

datAshur® personal

Remember to save your PIN in a safe place.

If lost or forgotten, there is no way to access the drive.

If you are having difficulty using your datAshur Personal® drive please contact our technical department at email address - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2014. All rights reserved.

Windows™ is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

N30732

All trademarks and brand names are the property of their respective owners

ClevX, LLC patents pending

iStorage datAshur Personal® is developed and manufactured by iStorage Ltd. and is based on DataLock® technology licensed from ClevX, LLC

Table of Contents

Introduction 4
Package contents 4
Layout 5
LED indicators and their actions 5
Customer delivery 5
How to change the User PIN 6
How to create a New User PIN - when all cryptographic parameters have been zeroed 6
Unlocking the drive with the User PIN 8
Locking the drive 8
Configuring the Admin PIN 8
How to unlock the drive with the Admin PIN 10
Changing the Admin PIN 11
Administrator Privilege Commands 12
i. Clear the User PIN: 12
ii. Enable write protect - read only mode: 12
iii. Disable write protect - read only mode: 12
iv. Show security controller firmware version: 13
How to reset the drive 14
Configuring the drive with Windows OS after a complete reset 14
Configure the drive with Mac OS 20
Brute Force Hacking Detection 22
Booting from the datAshur Personal 22
FAQ's - Frequently Asked Questions 23
Technical support & Warranty 27

Introduction

Thank you for purchasing the **iStorage** datAshur Personal® drive, an ultra secure and easy to use, hardware encrypted USB **PIN** activated flash drive.

The datAshur Personal® drive uses military grade AES 256-bit CBC hardware encryption, which encrypts all data stored on the drive in real-time. The datAshur Personal® drive requires no software and is OS and host independent.

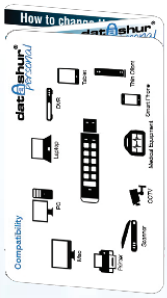
The datAshur Personal® drive incorporates a rechargeable battery allowing the user to enter a 7-15 digit **PIN** (Personal Identification Number) onto the on-board keypad before connecting the drive to a USB port.

Should the drive be lost or stolen, the user can rest assured that all data held on the datAshur Personal® drive is safe and cannot be accessed by any unauthorised person.

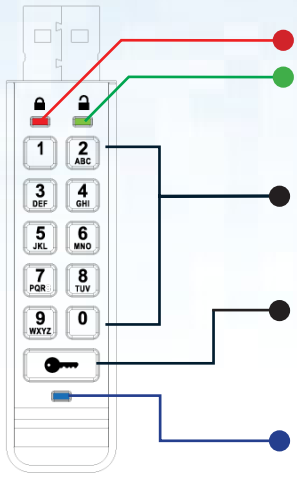
The datAshur Personal® drive can be configured with both a **User** and **Admin PIN**, making it perfect for corporate and government deployment. As the datAshur Personal® drive is unlocked via the onboard keypad and not a host computer, it is not vulnerable to software/hardware based key-loggers or brute force attacks.

Package contents

- datAshur Personal® USB flash drive
- Quick Start Guide



1. Layout



LOCK LED, stand by while the drive is locked
UNLOCK LED, drive is unlocked when flashing

Keypad

Key Button, used to activate the drive and to enter **PIN** codes

BLUE LED, when solid, the drive is connected to the computer, when flashing data is being transferred.

2. LED indicators and their actions

When all LEDs are OFF the datAshur Personal is locked and secure.				blink	Drive is locked and secure
	blink	Drive is unlocked in **User Mode**		solid	No **User PIN** is configured
	double blink	Drive is unlocked in **Admin Mode**	&	blink together	Accepting **User PIN** verification when setting / changing the **PIN**
	solid	Drive is connected to a powered USB port	&	double blink	Accepting **Admin PIN** verification when setting / changing the **PIN**
	solid	Drive is connected to host computer and is idle	&	illuminate together	Accepting new **PIN**
	blink	Data exchange with host computer	&	blink alternately	Error

3. Customer delivery

- datAshur Personal® is shipped with a default **User PIN** 1-1-2-2-3-3-4-4
- Rechargeable battery installed and charged
- **Admin PIN** is not set

4. How to change the User PIN

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers e.g. 3-3-3-3-3-3-3
- Must not contain only consecutive numbers e.g. (1-2-3-4-5-6-7),(7-8-9-0-1-2-3-4),(7-6-5-4-3-2-1)
- Drive must **NOT** be connected to a host

INSTRUCTIONS	LED ACTIVITY
Press **KEY Button**	& will blink together
Enter **User PIN** to unlock drive (Factory default **PIN** 1,1,2,2,3,3,4,4) and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Press and hold **KEY Button** for 3 seconds	& will illuminate together
While & illuminated enter **New User PIN** and press **KEY Button**	& will blink in unison
Re-enter **New User PIN** and press **KEY Button**	& will illuminate and then change to blinking
Insert datAshur Personal into USB port	**N.B.** blinks if 1st and 2nd entries match & blink alternately if **PIN** entry incorrect

Note: If a mistake was made while defining a new **PIN** or the procedure was aborted, the drive will retain the old **PIN**.

5. How to create a new User PIN

when all cryptographic parameters have been zeroed

All cryptographic parameters (including **User PIN** and **Admin PIN**) are zeroed after hacking detection has been triggered by 10 consecutive failed attempts to unlock, or when the drive has been manually reset (see section No. 12)

This state is evident by a solid lit **RED LED** indicator. It will be necessary to set a **New User PIN** by following these instructions.

Once the **User PIN** has been defined, a new encryption key is generated using the on-board random number generator.

Configuring a New User PIN overleaf

5. How to create a new User PIN - continued

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers e.g. 3-3-3-3-3-3-3-3
- Must not contain only consecutive numbers e.g. (1-2-3-4-5-6-7),(7-8-9-0-1-2-3-4),(7-6-5-4-3-2-1)
- Drive must **NOT** be connected to a host

INSTRUCTIONS	LED ACTIVITY
Press and hold **KEY Button** for 3 seconds	& will illuminate together
While & are illuminated enter a **New User PIN** and press **KEY Button**	& will blink in unison
Re-enter **New User PIN** and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Insert datAshur Personal into USB port	will illuminate in a constant state & blink alternately if **PIN** entry incorrect

Note:

It becomes necessary to format the drive at this point as all previous data is obscured with the previous encryption key (including the file allocation table).

A **User PIN** can only be created when the **RED LED** is lit in a constant state (datAshur Personal® reset) or changed when the **GREEN LED** is blinking (datAshur Personal® unlocked).

Neither **User** nor **Admin PIN** can be created while the drive is connected to a host computer.

6. Unlocking the drive with User PIN

All data stored on the drive is encrypted using AES 256-bit CBC encryption. In order to access, the drive must first be unlocked. A locked drive is not accessible by the host computer.

INSTRUCTIONS	LED ACTIVITY
Press **KEY Button**	& will blink together
Enter **User PIN** to unlock drive (Factory default **PIN** 1,1,2,2,3,3,4,4) and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Note that at this point the following occurs:	will blink indicating the correct **PIN** entry will blink indicating the incorrect **PIN** entry
Insert your datAshur Personal into USB port	will illuminate in a constant state will illuminate and flicker

Note: Once unlocked, the **GREEN LED** will blink for 30 seconds, within which time the drive needs to be connected to a USB port.
If no connection has been detected within 30 seconds the drive will lock.

7. Locking the drive

The datAshur Personal® drive automatically locks when unplugged from the host computer or power to the USB port is turned off.

8. Configuring the Admin PIN

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers e.g. 3-3-3-3-3-3-3-3
- Must not contain only consecutive numbers e.g. (1-2-3-4-5-6-7),(7-8-9-0-1-2-3-4),(7-6-5-4-3-2-1)
- Drive must **NOT** be connected to a host

If a **User PIN** exists, the datAshur Personal® drive must be unlocked with the **User's PIN** first.
If the drive is in a reset state (solid **RED** indicator), an **Admin PIN** can be set at any time.

For details please see the table overleaf.

The following table depicts the possible actions when the drive is in different states:

User PIN	Admin PIN	Possible Actions
NOT SET	NOT SET	Can set either **User** or **Admin PIN**
		Cannot access drive until **User** or **Admin PIN** is defined
SET	NOT SET	Can change **User PIN** when unlocked as User
		Can set **Admin PIN** when unlocked with **User PIN**
		Can access data when unlocked as User
NOT SET	SET	Can set **User PIN** when drive is locked
		Can unlock drive with **Admin PIN**
		Can change **Admin PIN** when unlocked as Administrator
		Can perform Administrator commands
SET	SET	Can unlock drive with either **User** or **Admin PIN**
		Can change **User PIN** when unlocked as User
		Can change **Admin PIN** when unlocked as Administrator

The drive has to be unlocked in user mode in order to proceed with configuring an **Admin PIN**.
It is set by following the instructions below:

INSTRUCTIONS	LED ACTIVITY
Double press the **KEY Button** and hold on the 2nd press for 3 seconds	& will double blink once and then turn solid
Enter the **New Admin PIN** and press **KEY Button**	& will double blink if correct **PIN** entry or will blink alternately if **PIN** entry incorrect
Re - Enter the **New Admin PIN** and press **KEY Button**	& will illuminate together for approximately 2 seconds and then: will double blink indicating correct **PIN** entry
Note that at this point the following occurs:	will double blink if 1st and 2nd entries match & will blink alternately if **PIN** entry incorrect
Insert your datAshur Personal into USB port	will illuminate in a constant state will illuminate and flicker

Note: A double blink indicates the drive is unlocked in Admin mode.
A single blink indicates the drive is unlocked in User mode.

Figure 1 shows the **GREEN** blinking characteristics when the drive is opened in user mode (top) and admin mode (bottom).

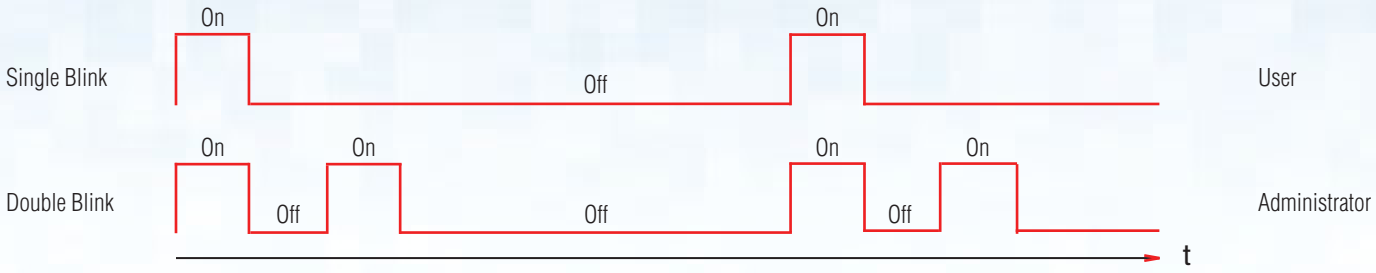


Figure 1: Mode indication

Figure 2 shows the difference between pressing **KEY Button** to set a **User PIN** vs. setting the **Admin PIN**.

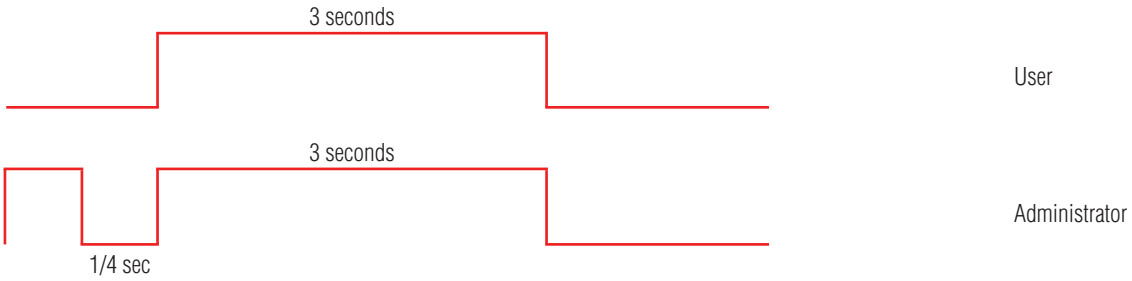


Figure 2: Key entry for mode selection

9. How to unlock with Admin PIN

INSTRUCTIONS	LED ACTIVITY
Press the **KEY Button** twice in succession (similar to double-clicking a mouse)	& will double blink together (Figure 1. above)
Enter **Admin PIN** Press **KEY Button**	& will illuminate together as self-tests are run will double blink if admin entered correct **PIN** will blink if incorrect **PIN** was entered

Note: Once unlocked, the **GREEN** **LED** will blink for 30 seconds, within which time the drive needs to be connected to a USB port.

If no connection has been detected within 30 seconds the drive will lock.

10. Changing the Admin PIN

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers e.g. 3-3-3-3-3-3-3-3
- Must not contain only consecutive numbers e.g. (1-2-3-4-5-6-7),(7-8-9-0-1-2-3-4),(7-6-5-4-3-2-1)
- Drive must **NOT** be connected to a host

Once an **Admin PIN** has been created, the datAshur Personal® must be unlocked with the **Admin PIN** first. If the drive is in a reset state (solid **RED** indicator), an **Admin PIN** can be set at any time.

INSTRUCTIONS	LED ACTIVITY
Press the **KEY Button** [key] [key] **twice** in succession (similar to double-clicking a mouse)	& will double blink together
Enter **Admin PIN** Press **Key Button** [key]	& will illuminate together as self-tests are run will double blink if admin entered correct **PIN** will blink if incorrect **PIN** was entered
Double press the **KEY Button** [key] [key] and hold on the 2nd press for 3 seconds	& will double blink once and then turn solid
Enter the **New Admin PIN** and press **KEY Button** [key]	& will double blink if correct **PIN** entry or will blink alternately if **PIN** entry incorrect
Re-enter the **New Admin PIN** and press **KEY Button** [key]	& will illuminate together for approximately 2 seconds and then: will double blink indicating correct **PIN** entry
Note that at this point the following occurs: →	will double blink if 1st and 2nd entries match & will blink alternately if **PIN** entry incorrect
Insert your datAshur Personal into USB port	will illuminate in a constant state will illuminate and flicker

Note: **GREEN LED** will double blink for 30 seconds, within which time the drive needs to be connected to a USB port.

If no connection has been detected within 30 seconds, the drive will lock.

11. Administrator Privilege Commands

A number of special functions can be performed once the drive is unlocked in administrator mode.

FUNCTION	BUTTON COMBINATION	OUTCOME
i. Clear the **User PIN**	**U** + **R** + **KEY Button**	User PIN **RESET**
ii. Turn write protect **ON**	**W** + **P** + **1** + **KEY Button**	Write Protect **ON**
iii. Turn write protect **OFF**	**W** + **P** + **0** + **KEY Button**	Write Protect **OFF**
iv. Show firmware version	**R** + **V** + **KEY Button**	Revision

Each of the commands above can only be performed with the drive unlocked in admin mode.

i. Clear the User PIN:

In the event of a forgotten **PIN**, the Administrator can reset the **User PIN**.
This is done by performing the following:

- Unlock the drive in admin mode
- Double press and hold **KEY Button** as if changing the **Admin PIN**
- Enter '**U**' + '**R**' followed by **KEY Button** (e.g. **8 - 7 - KEY**)
- The **GREEN** and **RED LEDS** will blink 3 times to indicate success
- The **GREEN LED** will then double blink until plugged in
- After the drive re-locks, it will awake with a solid **RED LED**
- A new **User PIN** can be defined at this point

ii. Enable write protect - read only mode:

It is possible to write content to the drive as an administrator and restrict access to read-only.
This is done by performing the following:

- Unlock the drive in admin mode
- Double press and hold the **KEY Button** as if changing the **Admin PIN**
- Enter '**W**' + '**P**' + '**1**' followed by **KEY Button** (e.g. **9 - 7 - 1 - KEY**)
- **GREEN** and **RED LEDS** will blink 3 times to indicate success
- **GREEN LED** will then double blink until plugged in

Once activated, access is limited to read-only until write protect is disabled.
Note: **Write Protect** – read only mode is disabled on a reset of the datAshur Personal.

iii. Disable write protect - read only mode:

Restricted write protect access can be turned off with access restored to read / write.
This is done by performing the following:

- Unlock the drive in admin mode
- Double press and hold the **KEY** Button as if changing the **Admin PIN**
- Enter '**W**' + '**P**' + '**0**' followed by **KEY** Button (e.g. **9 - 7 - 0 - KEY**)
- **GREEN** and **RED LEDS** will blink 3 times to indicate success
- **GREEN LED** will then double blink until plugged in

Note: Also **Write Protect** – read only mode is disabled on a reset of the datAshur Personal.

11. Administrator Privilege Commands - continued

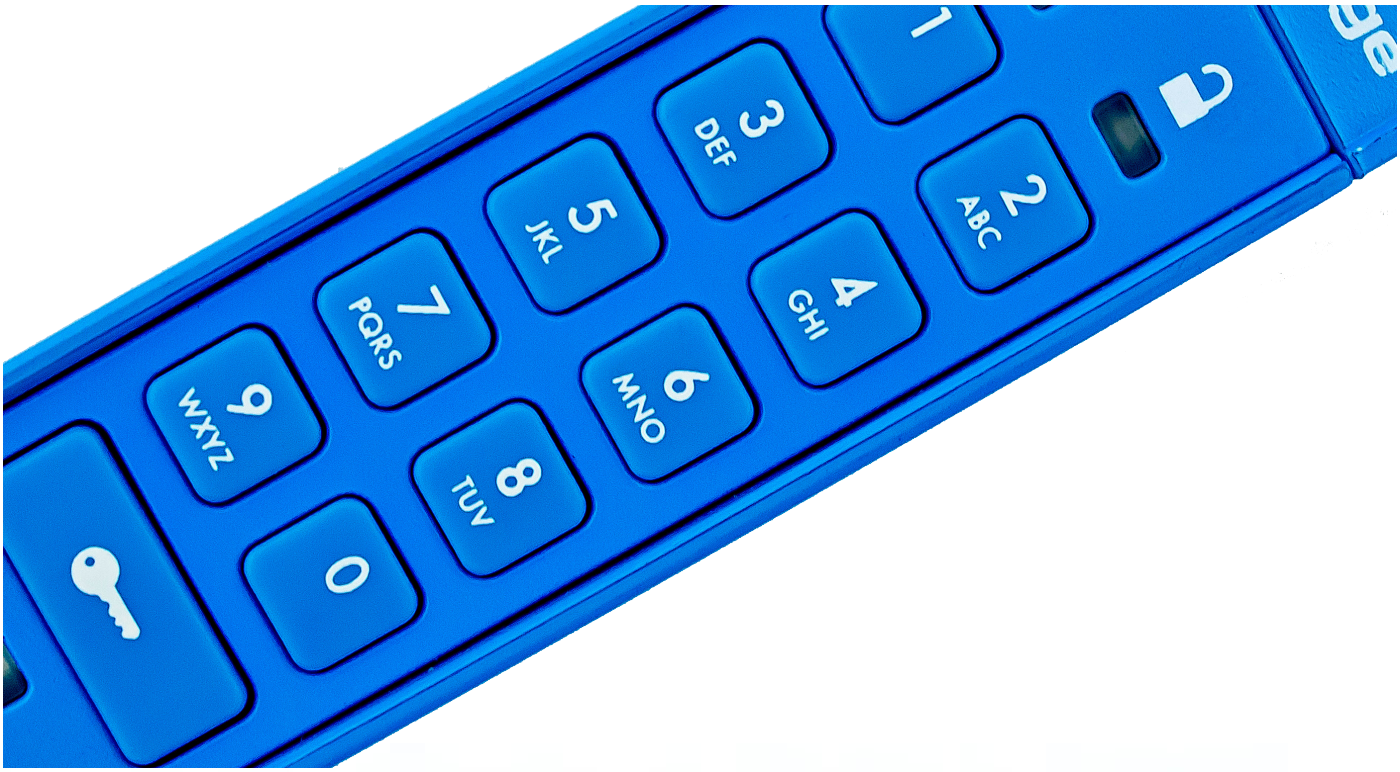
iv. Show security controller firmware version:

To display the firmware revision do the following:

- Unlock the drive in admin mode
- Double press and hold the **KEY Button** as if changing the **Admin PIN**
- Enter '**R**' + '**V**' followed by the **KEY Button** (e.g. **7 - 8 - KEY**)
- The **RED LED** will blink according to the most-significant digit of revision.
- The **GREEN LED** will blink according to the least-significant digit.

For example, if the revision number is '13', all indicators will turn off momentarily followed by a **1** (one) blink from the **RED LED** followed by **3** (three) blinks from the **GREEN LED**.

The drive will then start double blinking to indicate that it is unlocked in admin mode.



12. How to RESET the drive

In the event both **Admin** and **User PIN** have been forgotten, or user wants to delete all stored data, please follow the instructions below:

The reset process will clear all cryptographic parameters including both **User** and **Admin PIN**.

In addition, the write protect feature will be reset so the drive becomes writable again.

INSTRUCTION	LED ACTIVITY
Press and hold **KEY Button** & number button together for 3 seconds	& will illuminate together
Release buttons	& will blink in unison
Enter 9 9 9	& will blink in unison
Press **KEY Button**	& will turn off
Press **KEY Button**	will remain in solid state Indicates **User PIN** must be set prior to use

Defining a new **PIN** (either **User** or **Admin**) from the reset state will cause the datAshur Personal® to invoke the random number generator to create a new encryption key.

Once a new **PIN** is defined, the drive will become busy running self-tests and generating a new random encryption key.

This phase is evident by both the **RED** and **GREEN** **LEDS** intensifying in brightness.

The **GREEN** **LED** will blink when the drive is ready for use.

13. Configuring the drive with Windows OS after a complete reset

In the event that hacking detection has been triggered by entering the **incorrect PIN 10 times** in succession or the drive has been **reset**, all **data on the drive will be lost forever**.

Once a new **User PIN** has been created, the datAshur Personal® drive will need to be initialised and formatted.

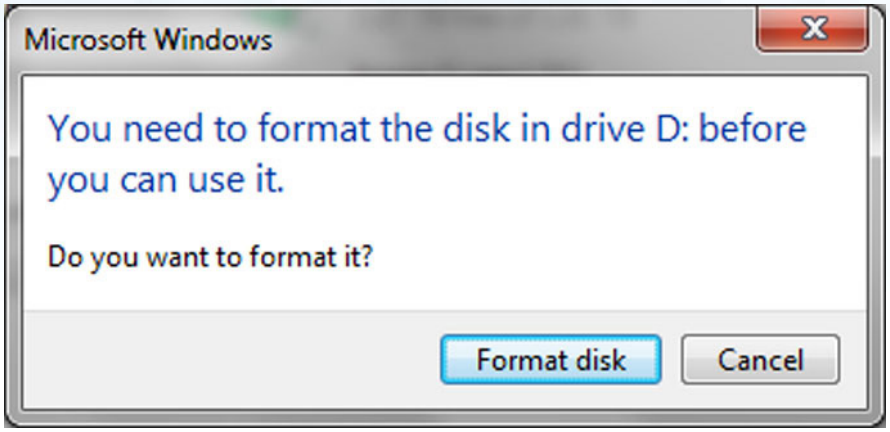
To initialise your datAshur Personal® drive, do the following:

1. Create a new **User PIN** (see section 5 above) in the **iStorage** datAshur Personal® **Manual**
2. Unlock the datAshur Personal® drive by entering the **New User PIN** and connect to a computer's USB port.

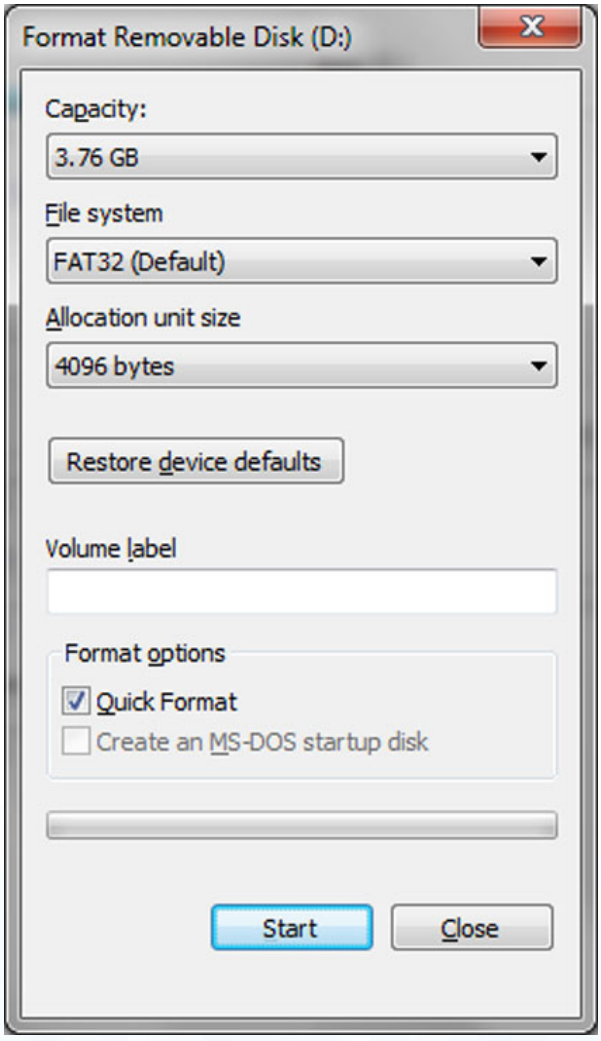
Action continued overleaf.

13. Configure the drive with Windows OS - continued

3. The computer should notify the user with the following message:

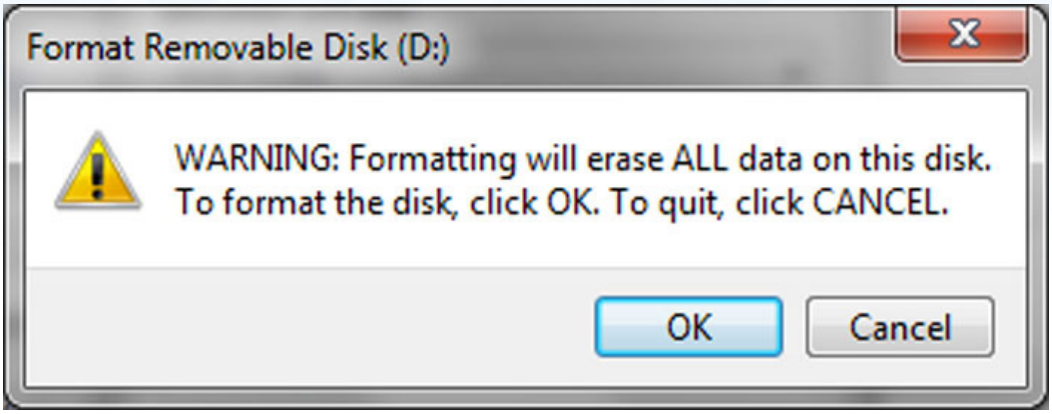


4. Proceed by clicking on **Format** disk.
   Select **FAT32** or **NTFS** depending on your needs, enter a **Volume Label** and click **Start**.



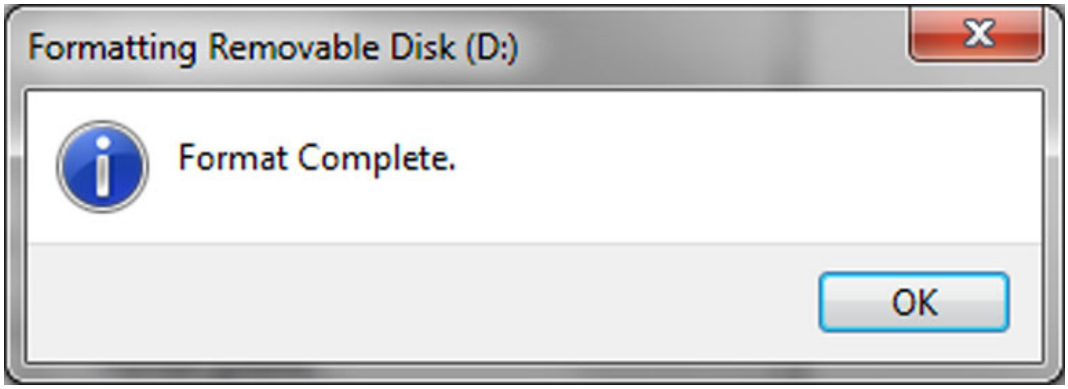
13. Configure the drive with Windows OS - continued

5. Click **OK** to continue with formatting the drive. **This procedure will erase ALL data on the drive**.


Format Removable Disk (D:)
WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.
OK
Cancel

6. The procedure will finish formatting the drive and confirm that formatting has been completed.

   While the datAshur Personal® drive is formatting the **BLUE LED** will be flashing.

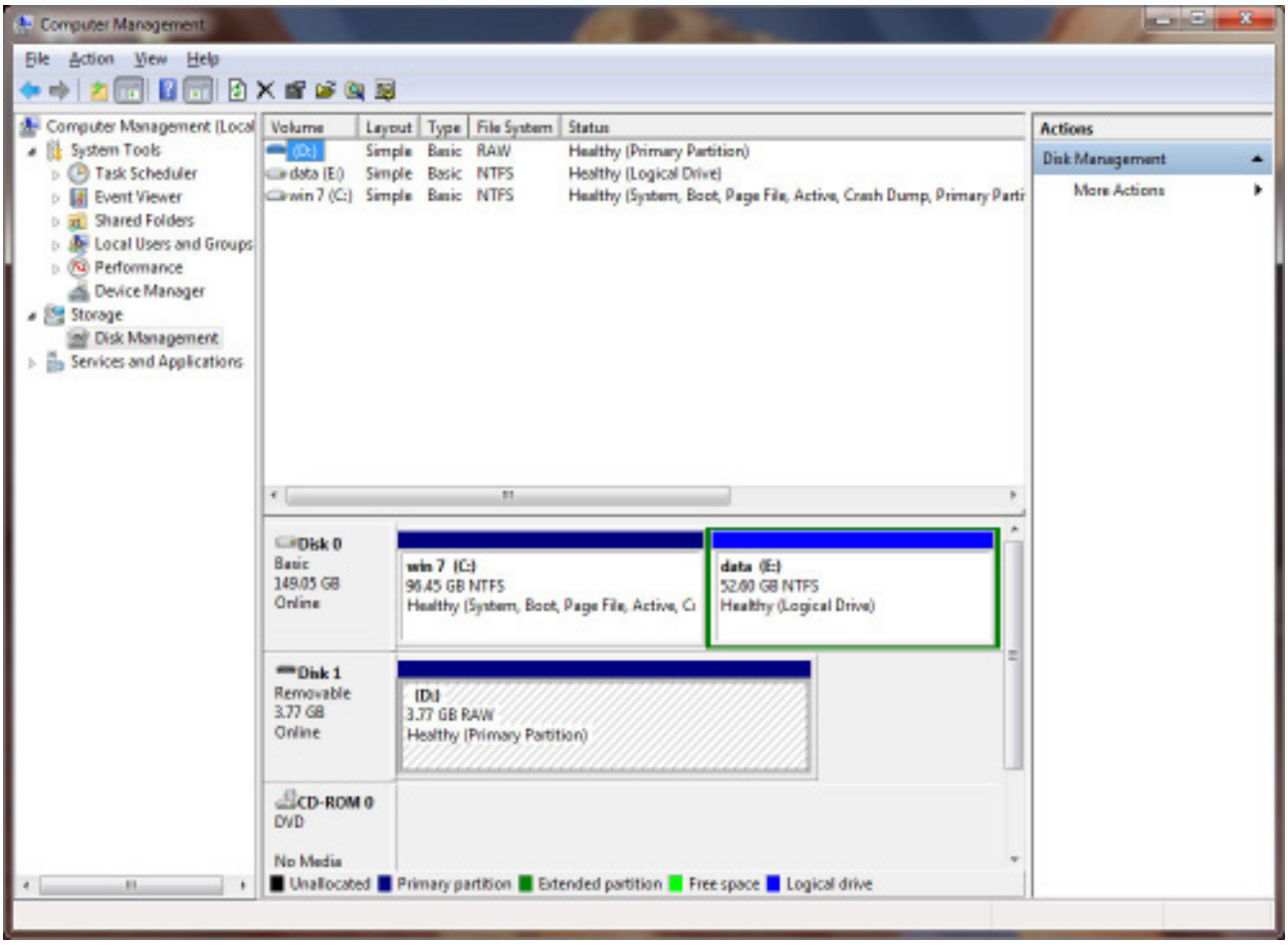


Once finished, the **BLUE LED** becomes solid and your datAshur Personal® drive is ready for use.

13. Configure the drive with Windows OS - continued

In case that the formatting wizard does not appear, please follow the procedure below:

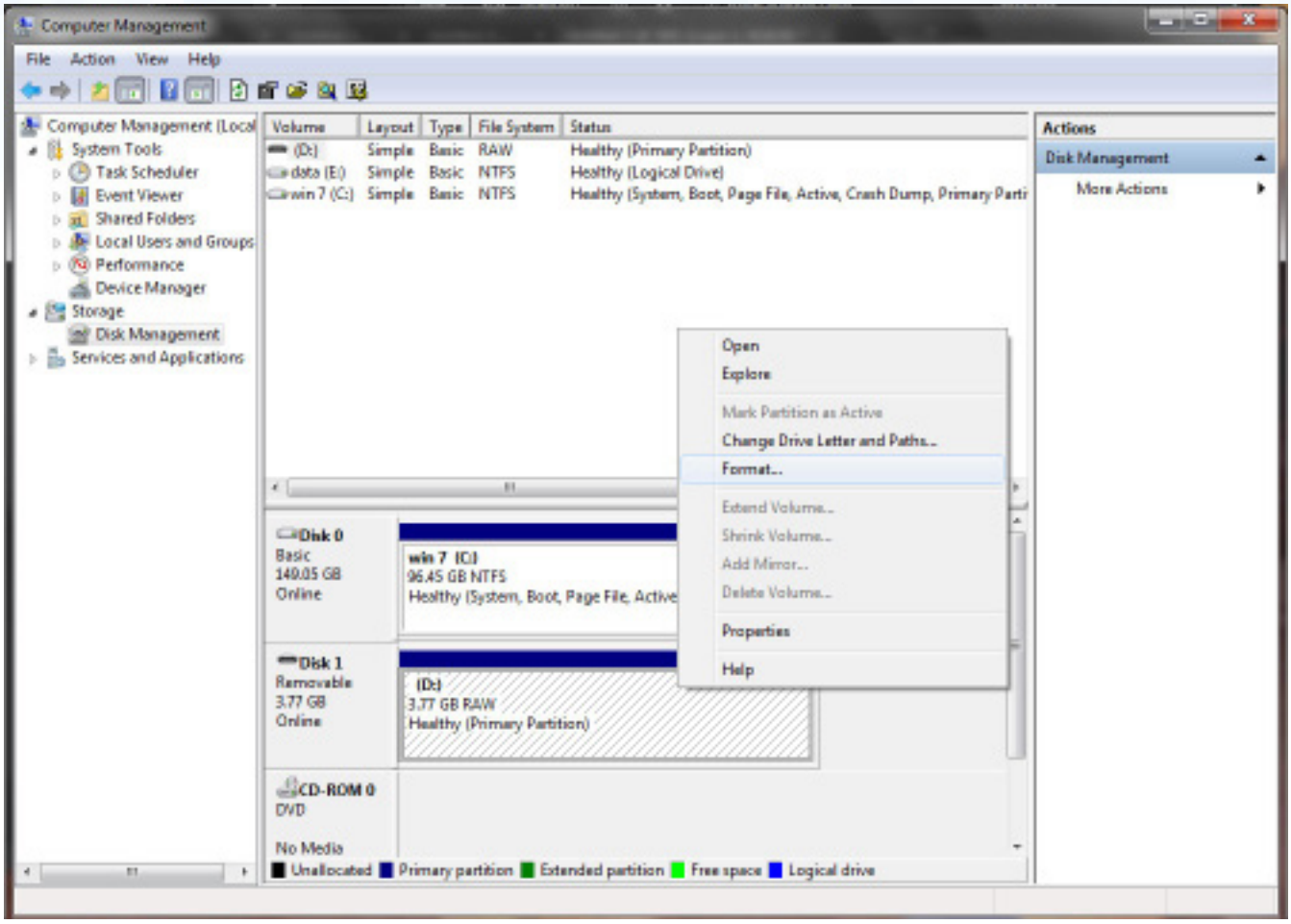
1. Right click **My Computer** or **Computer** and then click **Manage**.
2. In the Computer Management window under the **Disk Management** tab, the datAshur Personal® drive is recognised as a removable device in raw format.



Action continued overleaf.

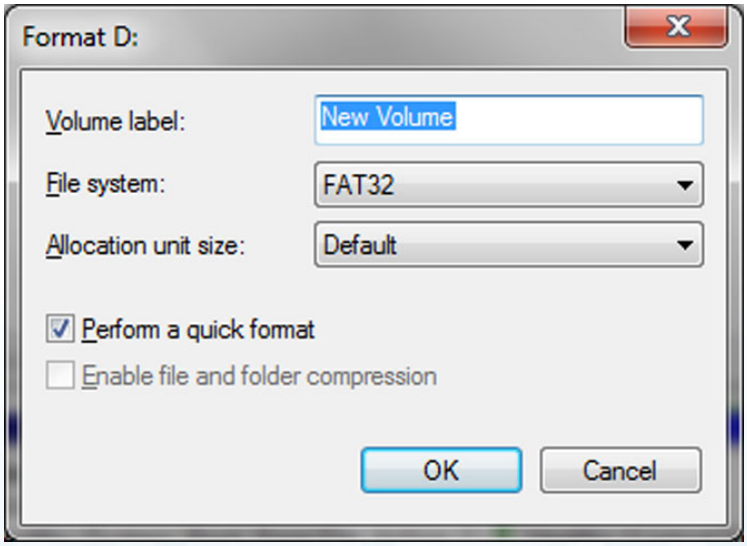
13. Configure the drive with Windows OS - continued

3. In the blank area under the unallocated section right click **Removable Raw Drive** and select **Format**



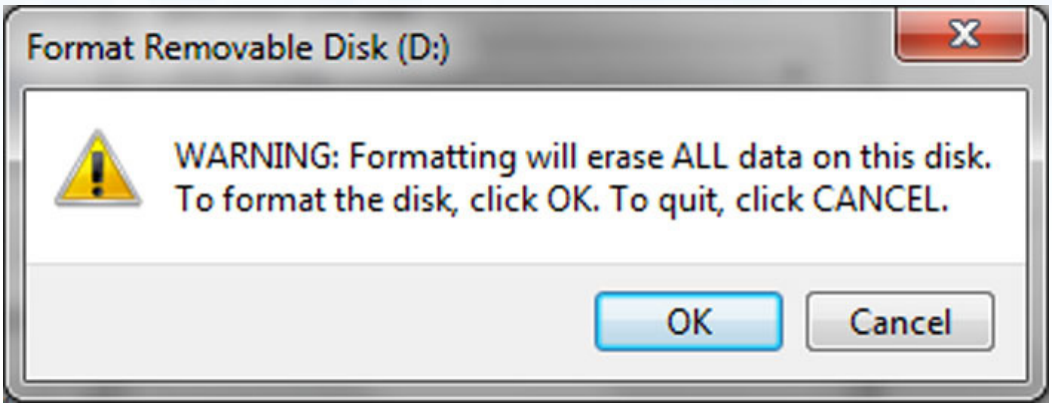
4. The **Format** window will open.

   Enter a new **Volume Label**.
   Select **FAT32** or **NTFS** depending on your needs and click **OK**.



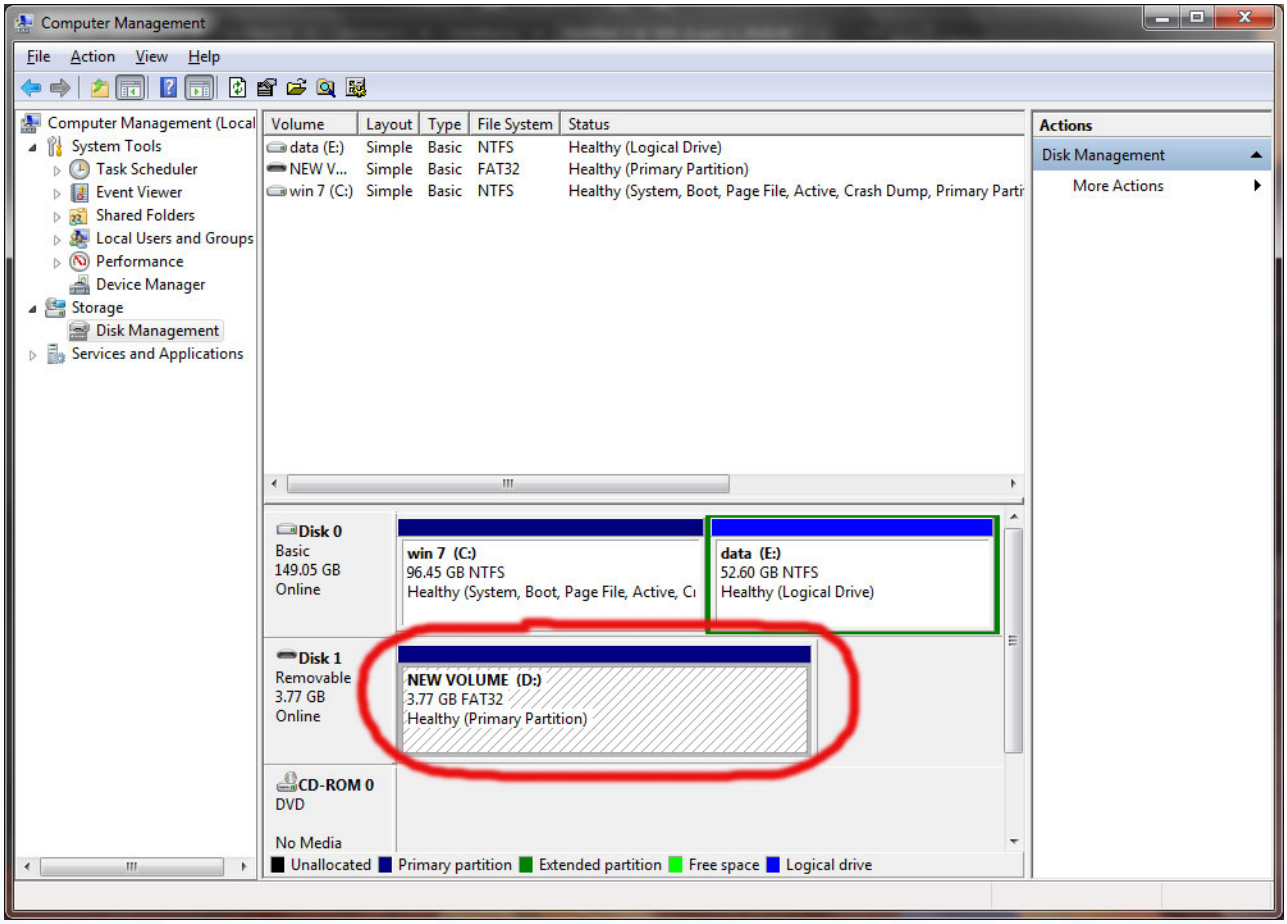
13. Configure the drive with Windows OS - continued

5. Click **OK** on the **Format** warning window to continue with formatting the drive.
   This procedure will erase ALL data on the drive.


Format Removable Disk (D:)
WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.
OK
Cancel

6. The procedure will finish formatting and return to the **Disk Management** window.

   While the datAshur Personal® drive is formatting the **BLUE LED** will start flashing.



When finished, the **BLUE LED** becomes solid and your datAshur Personal® drive is ready for use.

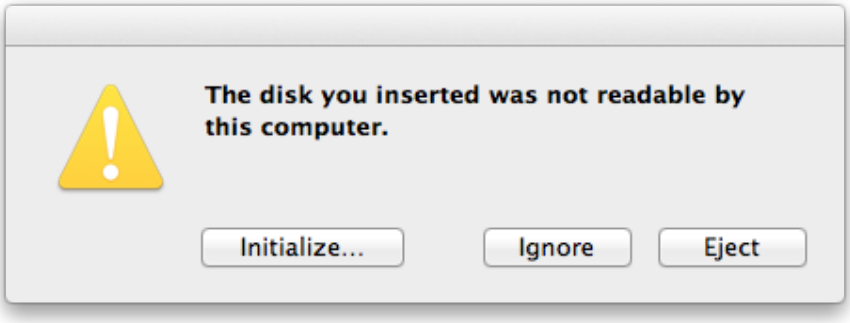
14. Configure the drive with Mac OS

In the event that hacking detection has been triggered by entering the **incorrect PIN 10 times** in succession or the drive has been reset, all **data on the drive will be lost forever**.

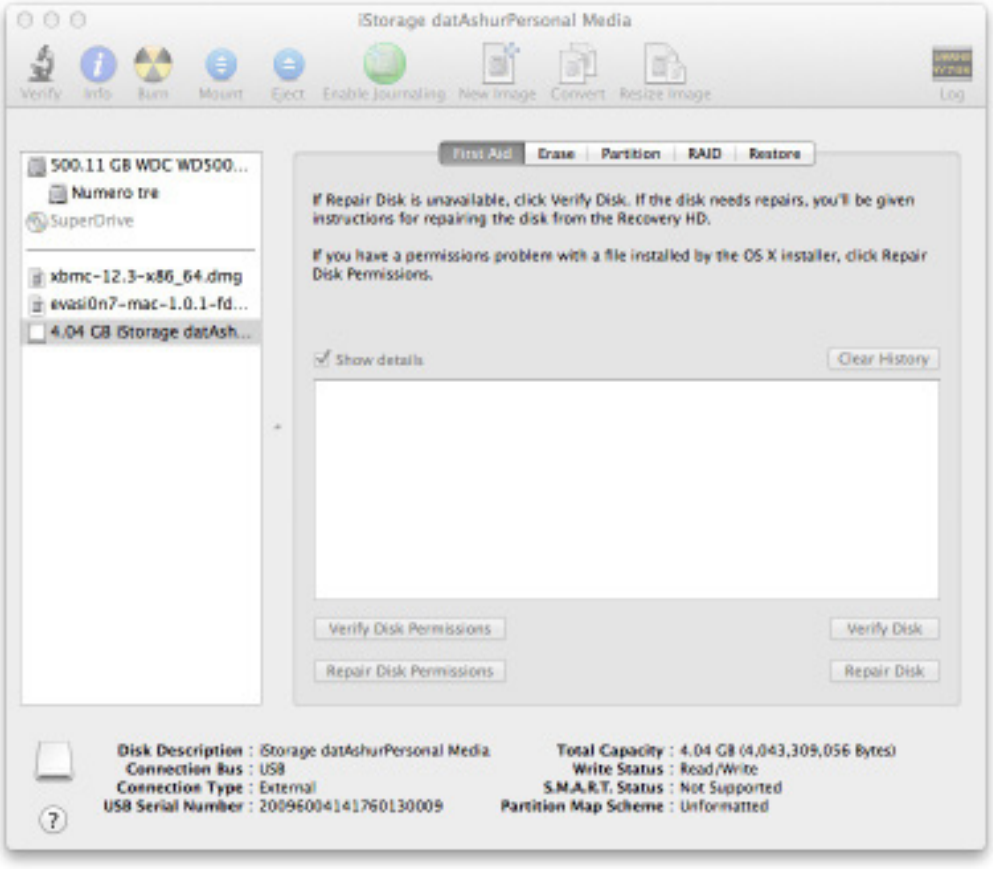
Once a **New User PIN** has been created, the datAshur Personal® drive will need to be initialised and formatted.

To format your datAshur Personal® drive on Mac OS computers, do the following:

1. Create a **New User PIN** (see section No. 5)
2. Unlock the datAshur Personal® drive by entering the **New User PIN** and connect to a Mac computer's USB port.
3. The system will prompt you with **INITIALIZE** window.



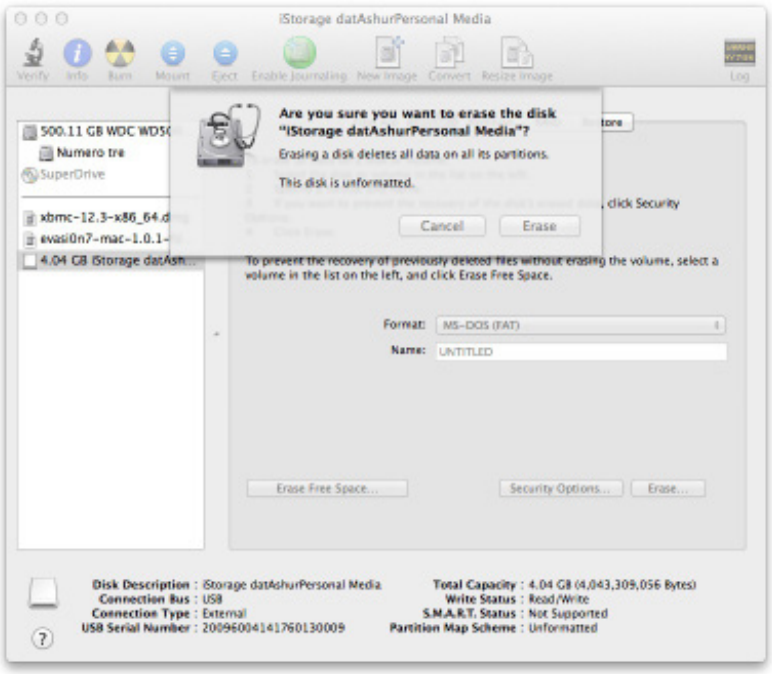
4. Press **INITIALIZE** and select the datAshur Personal® drive in the Disk Utility window.



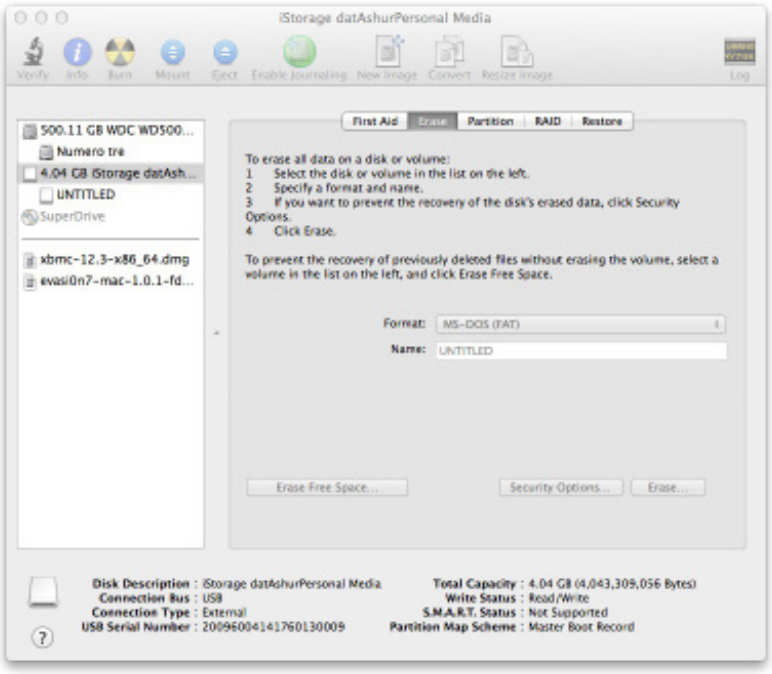
14. Configure the drive with Mac OS - continued

To format your datAshur Personal® drive on Mac OS computers, do the following:

5. Click on the datAshur Personal® drive on the left side of the **Disk Utility** window.
6. Choose **Erase** from the contextual menu on the right side of the window
7. Select **MS-DOS** for the **Volume Format**
8. Click **Erase**


iStorage datAshurPersonal Media
Are you sure you want to erase the disk "iStorage datAshurPersonal Media"?
Erasing a disk deletes all data on all its partitions.
This disk is unformatted.
Cancel
Erase
Format: MS-DOS (FAT)
Name: UNTITLED
Erase Free Space...
Security Options...
Erase...
Disk Description : iStorage datAshurPersonal Media
Connection Bus : USB
Connection Type : External
USB Serial Number : 20096004141760130009
Total Capacity : 4.04 GB (4,043,309,056 Bytes)
Write Status : Read/Write
S.M.A.R.T. Status : Not Supported
Partition Map Scheme : Unformatted

9. The formatted datAshur Personal® drive will appear in the **Disk Utility** window and will mount onto the desktop.


iStorage datAshurPersonal Media
First Aid
Erase
Partition
RAID
Restore
To erase all data on a disk or volume:
1 Select the disk or volume in the list on the left.
2 Specify a format and name.
3 If you want to prevent the recovery of the disk's erased data, click Security Options.
4 Click Erase.
To prevent the recovery of previously deleted files without erasing the volume, select a volume in the list on the left, and click Erase Free Space.
Format: MS-DOS (FAT)
Name: UNTITLED
Erase Free Space...
Security Options...
Erase...
Disk Description : iStorage datAshurPersonal Media
Connection Bus : USB
Connection Type : External
USB Serial Number : 20096004141760130009
Total Capacity : 4.04 GB (4,043,309,056 Bytes)
Write Status : Read/Write
S.M.A.R.T. Status : Not Supported
Partition Map Scheme : Master Boot Record

15. Brute Force Hacking Detection

After 10 consecutive failed attempts to unlock the drive, all cryptographic parameters are zeroed including **User** and **Admin PIN**. In this state, a **New User PIN** must be defined which will cause a new encryption key to be generated.

All previously stored data is no longer accessible and the drive will require formatting.

16. Booting from the datAshur Personal®

iStorage datAshur Personal® USB drives are equipped with a 10 second delay in order to accommodate power cycling during a host boot process. No special actions are required on the part of the user. In order to use this feature, simply unlock the drive and connect to the USB port of a host computer. Turn on host power.

Under certain conditions, the drive may take 10 seconds to lock. For example, putting the host computer into standby mode and leaving the drive connected. To force an immediate lock, always unplug to remove USB power to the drive.

17. FAQ - Frequently Asked Questions

NOTE We strongly recommend that you carefully read this **User Manual**, shipped with the device or available for download on our website before contacting us for technical support.

There are no "**Back Doors**" to our products, we cannot retrieve a forgotten **PIN** or retrieve any data off the drives unless the **PIN** is known.

Below are answers for the most frequently asked questions:

Q. HOW DO I USE THE datAshur Personal® DRIVE FOR THE FIRST TIME?

A. The datAshur Personal® drive comes with a default **PIN CODE** which will unlock the device for the first time, allowing the user to create their own unique **User** and **Admin PIN**.

Please follow this procedure:

Press **KEY Button**
Enter **1-1-2-2-3-3-4-4**
Press **KEY Button**
The **GREEN LED** light will indicate the device is unlocked

Q. WHAT IS A USER PIN CODE?

A. The **User PIN** (Personal Identification Number) can be changed to almost any number that is desired.

To create your New User PIN follow the instructions below:

The **New User PIN** must be 7 to 15 digits long.
The **New User PIN** cannot contain only repetitive numbers (3-3-3-3-3-3-3)
The **New User PIN** cannot contain only consecutive numbers (1-2-3-4-5-6-7) , (7-6-5-4-3-2-1)

You can create a word, name, phrase or any other alphanumerical **PIN** combination by simply pressing the key with the corresponding letters on it.

Examples of these types of **PIN CODES** are:

For **Password1** you would press the following keys:
7(p**q**rs) **2**(a**b**c) **7**(pq**r**s) **7**(pq**r**s) **9**(**w**xyz) **6**(mn**o**) **7**(pq**r**s) **3**(**d**ef) **1**

For **iStorage** you would press:
4(gh**i**) **7**(pq**r**s) **8**(**t**uv) **6**(mn**o**) **7**(pq**r**s) **2**(a**b**c) **4**(**g**hi) **3**(d**e**f)

Using this method, long and easy to remember **PIN CODES** can be created.

17. FAQ - Frequently Asked Questions - continued

Q. HOW DO I UNLOCK THE datAshur Personal® DRIVE IF THE BATTERY IS DEAD?

A. Your datAshur Personal® drive has a built-in rechargeable battery.

Even if the battery is fully discharged you can still continue to use the drive by following the instructions below:

Connect the datAshur Personal® drive to a USB port on any computer
While connected to the computer, enter the **User** or **Admin PIN** to unlock the drive
While connected to the USB port, the internal battery will automatically charge - this is shown by a flashing **BLUE LED**.

We recommend you keep the datAshur Personal® drive connected for approximately 1 hour to fully charge the battery.

Q. HOW DO I CHANGE THE DEFAULT PIN CODE?

A. Please follow this procedure:

Press the **Key Button**
Within 10 seconds enter the **Current User PIN** and press the **Key Button** again
Press and hold the **Key Button** for 3 seconds
Enter a **New User PIN** number (The **PIN** must be 7 - 15 digits long)
Press the **Key Button** to store the **New User PIN**
Re-enter the **New User PIN** number
Press the **Key Button** to confirm the **New User PIN** .

Q. WHAT IF I FORGET MY PIN CODE ON MY datAshur Personal® DRIVE?

A. If you forget the **User** and **Admin PIN**, there is absolutely no way of gaining access to the data stored on the drive, there are no back doors into the drive.
You will need to completely reset the datAshur Personal® drive by following the directions in this **User Manual**. By resetting the drive, all data stored on the datAshur Personal® will be deleted.

When the datAshur Personal® drive **is reset the following occurs:**

- A new encryption key is generated
- The **User** and **Admin PIN** are deleted
- All the data on the datAshur Personal® drive is deleted
- A new **User PIN** will need to be set
- The datAshur Personal® drive will need to be formatted

17. FAQ - Frequently Asked Questions - continued

Q. HOW DO I CREATE AN ADMIN PIN?

A. The **Admin PIN** is useful in a corporate environment where an Administrator can provide access to the datAshur Personal® drive if the **User PIN** is forgotten or unavailable.

Please follow this procedure:

Press the **Key Button**
Enter the **User PIN** within 10 seconds and press the **Key Button**
Rapidly press the **Key Button** twice and hold the **Key Button** on the second press for 4 seconds
Enter a new **Admin PIN** and press the **Key Button**

NOTE If the **LEDS** in the above step are "single blinking" then the first key press did not register or was not fast enough.
If you continue, you will be changing the **User PIN**
Re-enter the **New Admin PIN** and press the **Key Button**

Q. WHAT IS BRUTE FORCE OR HACKING ATTEMPT PROTECTION?

A. 10 consecutive incorrect **PIN** entries will activate the brute force mechanism and will completely reset the drive as follows:

- A new encryption key is generated
- The **User** and **Admin PIN** are deleted
- All the data on the datAshur Personal® drive is deleted
- A new **User PIN** will need to be set
- The datAshur Personal® drive will need to be formatted

Q. HOW DO I RESET THE datAshur Personal® DRIVE?

A. In case the **User PIN** is forgotten, or if you would like to delete all data stored on the drive and configure a **New User PIN,** the **RESET** process will clear the **User** and **Admin PIN,** the encryption key and will destroy all data. This means a **New User PIN** will have to be defined in order to re-enable the datAshur Personal® drive.

Also, since this forces the creation of a new encryption key, the datAshur Personal® drive will have to be reformatted.

Please follow this procedure:

Press and hold the **Key Button** and the number **2 Button** for 3 seconds
Press **9** - **9** - **9** and press the **Key Button**
Press the **Key Button** again

NOTE When the solid **RED LED** is on, a **New User PIN** will need to be set.

17. FAQ - Frequently Asked Questions - continued

Q. HOW DO I CREATE A NEW USER PIN AFTER RESETTING THE datAshur Personal® DRIVE?

A. Once the datAshur Personal® drive has been reset either with the method from the previous step or from a brute force attack (10 unsuccessful attempts to unlock) a **New User PIN** will need to be defined.

Please follow this procedure:

Press and hold the **Key Button** for 3 seconds
Within 10 seconds enter the **New User PIN**
Press the **Key Button** to save
Re-enter the **New User PIN** number & press the **Key Button**
If the **New User PIN** was accepted, the **GREEN LED** will be flashing.

The datAshur Personal® drive will be unlocked and be ready to format.

Q. HOW SHOULD I FORMAT MY DRIVE?

A. The datAshur Personal® drives come formatted to **FAT32** filing system by default. This will allow you to use the datAshur Personal® drive across all platforms (Windows, Apple, Linux) with a file size limitation of up to 4GB.

Q. WHAT IS THE DIFFERENCE BETWEEN THE USER MODE AND ADMIN MODE?

A. For an ordinary user we recommend to have just one **PIN** code, whereas in a corporate environment we strongly suggest creating an **Admin PIN** and **User PIN**.
When in admin mode you will be able to change the **User PIN** code.

Q. HOW DO I ACCESS ADMIN MODE?

A. Please follow this procedure:

Press the **Key Button** 2 times
Within 10 seconds enter the **Admin PIN**
Connect the datAshur Personal® drive to a USB port within 30 seconds

18. Techical Support

iStorage provides the following helpful resources for you:

iStorage's Website
http://www.istorage-uk.com

E-mail correspondence
support@istorage-uk.com

Telephone support with our Technical Support Department on +44 (0) 20 8991-6260.
iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m.
GMT - Monday through Friday.

Warranty and RMA information

Three Year Warranty

iStorage offers a 3-year warranty on the iStorage datAshur Personal® against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from **iStorage** or an authorised reseller.

Disclaimer and terms of the warranty:

THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.
ISTORAGE WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF ISTORAGE.
THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM ISTORAGE OR AN AUTHORIzED RE-SELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLECT, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE: 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY ISTORAGE; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN ISTORAGE AND SHALL BE VOID.
THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.
NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF ISTORAGE OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.
ISTORAGE SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSE-QUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT ISTORAGE WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

iStorage Limited, iStorage House,
13 Alperton Lane, Perivale, Middlesex, UB6 8DH
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com